U.S. Department of Justice

United States Attorney
Eastern District of New York

WMP:CAO/CLN/RMT
F.#2012R00103

271 Cadman Plaza East
Brooklyn, New York 11201

August 11, 2015

BY HAND DELIVERY AND ECF

The Honorable Raymond J. Dearie
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Vitaly Korchevsky et al.,
Criminal Docket No. 15-381 (RJD)

Dear Judge Dearie:

The government respectfully submits this letter memorandum in support of its request for permanent orders of detention for the defendants Vitaly Korchevsky, Leonid Momotok and Alexander Garkusha. On August 5, 2015, a grand jury in the Eastern District of New York returned an indictment charging the defendants with conspiring to commit wire fraud; conspiring to commit securities fraud; two counts of substantive securities fraud; and conspiring to commit money laundering. For the reasons set forth below, the defendants present a substantial risk of flight. Therefore, the government respectfully requests that the Court enter orders of detention for the defendants.

This request is based upon: (a) the disturbing nature and circumstances of the defendants' crimes; (b) the overwhelming evidence of the defendants' guilt; and (c) the vast financial resources available to the defendants and their co-conspirators, including assets in multiple foreign countries, as well as the defendants' personal ties to non-extradition countries.

FACTUAL BACKGROUND

I. Overview of the Scheme

The defendants' scheme was highly complex, spanning multiple continents and employing sophisticated means of computer intrusion and securities trading. It also was enormously profitable. The investigation, to date, has revealed that the defendants and their co-conspirators made at least $30 million in illegal profits.

As described in greater detail in the indictment, the defendants and their co-conspirators unlawfully traded in U.S. public companies' stocks based on material nonpublic information ("MNPI") that was obtained through unauthorized computer intrusions (or "hacking") into the computer servers of newswire companies such as PR Newswire Association ("PR Newswire"), Marketwired L.P. ("Marketwired") and Business Wire (collectively, the "Victim Newswires").

These Victim Newswires act as repositories for their clients' MNPI for a brief window of time before the client companies are ready to publicize it. The defendants and their co-conspirators stole the MNPI by hacking into the Victim Newswires' servers during the window of opportunity between the companies' upload of press releases onto the newswire services' servers and the public disclosure of those releases, and then traded on the MNPI within that window of time (hereinafter referred to as "within the window" or "inside the window" trades). Forensic analysis of compromised computer media and the defendants' trading activity has revealed that these hacks began in at least 2010.

The defendants and their co-conspirators were organized into three groups: (1) the co-conspirators who hacked the Victim Newswires and stole MNPI (including Ivan Turchynov and Oleksandr Ieremenko ("Co-Conspirator 4" and "Co-Conspirator 5" in the indictment, respectively)); (2) the co-conspirators who traded on the hacked MNPI (including the defendants Vitaly Korchevsky, Vladislav Khalupsky, Leonid Momotok and Alexander Garkusha, together with co-conspirators including Arkadiy Dubovoy and Igor Dubovoy ("Co-Conspirator 1" and "Co-Conspirator 2" in the indictment, respectively) (collectively, the "Traders"); and (3) the co-conspirators who communicated between the Hackers and the Traders (such as Pavel Dubovoy ("Co-Conspirator 3" in the indictment)) (the "Middlemen"). The Hackers used deceptive means to hack into the newswires and steal undisclosed press releases. The Traders then traded on the MNPI contained in the stolen press releases, sharing the profits with the Hackers through bank accounts throughout the world.

All told, between January 2011 and February 2014 alone, the defendants and their co-conspirators stole more than 100,000 press releases and executed at least 1,000 inside the window trades based on MNPI stolen from the Victim Newswires resulting in more than $30 million in illegal profits from this international scheme. The stolen MPNI pertained to well-known U.S. companies such as Boeing, Hewlett Packard, Foot Locker and Caterpillar.

II. The Evidence

The government's investigation, led by the Federal Bureau of Investigation and the U.S. Secret Service, has uncovered massive amounts of evidence regarding the means by which the Victim Newswires were hacked, the scope and coordination of the unlawful trading, and the various means of communication employed by the defendants and their co-conspirators to coordinate the dissemination of the MNPI and the trading in order to maximize the scheme's profitability. The investigation has also uncovered evidence of the

defendants and their co-conspirators laundering and transferring millions of dollars of illicit profits to Europe, Asia and elsewhere through the use of shell companies.

A. Evidence of the Hacks of the Victim Newswires

The Hackers attempted to gain access to the Victim Newswires' computer networks to steal MNPI using various methods, such as phishing[1] attempts and the surreptitious infiltration of servers the Victim Newswires leased from data storage providers.

In July 2010, the Hackers gained access to PR Newswire through the use of malware.[2] The Hackers sent unauthorized PHP[3] commands to the PR Newswire servers. Through these and other techniques, the Hackers could access press releases maintained on PR Newswire's network from any Internet-connected computer in the world. Once the Hackers accessed the PHP script, they were able to maneuver freely on PR Newswire's computer network, including accessing the confidential press releases of the companies that used PR Newswire. Web server logs recovered from the hacked PR Newswire servers show repeated and regular improper accesses to the PR Newswire servers. On October 10, 2012, Ieremenko sent a message, in Russian, to an unidentified individual, which stated, "I'm hacking prnewswire.com." When PR Newswire identified and removed malware that the Hackers had installed on its servers, an IP address associated with Turchynov made several unauthorized attempts to regain access to the PR Newswire servers.

Forensic exploitation of computer media seized by law enforcement officials in the Ukraine provided evidence that the Hackers also gained unauthorized access to Business Wire's servers. For example, a computer belonging to Ieremenko contained a file listing user IDs and associated hashed passwords for more than 200 employees of Business Wire. In addition, on March 25, 2012, in an Internet chat between Turchynov and Ieremenko, Ieremenko stated that he had successfully "bruted"[4] a number of hashed passwords. The next

[1] "Phishing" refers to an attempt to gain unauthorized access to a computer or computers by sending an email that appeared to be a legitimate communication from a trustworthy source, but contained malware or a link to download malware.

[2] "Malware" refers to malicious computer software programmed to, inter alia, gain and maintain unauthorized access to computers and to identify, store and export information from hacked computers.

[3] "PHP script" is a server-side scripting language designed for web development but also used as a general-purpose programming language. An unauthorized PHP script is an unauthorized program that can run undetected within a hacked server.

[4] "Brute force attacks" or "bruting" refers to one method for decrypting data. This method could be used to decrypt a password hash, revealing the unencrypted password.

day, Ieremenko sent Turchynov an electronic communication containing a link to malware that had been placed on Business Wire's computer network.

The government's investigation has also uncovered evidence that beginning in at least February 2010, the Hackers gained unauthorized access to press releases on Marketwired's networks using a series of SQL injection[5] attacks. For example, between approximately April 24, 2012 and July 20, 2012, Turchynov sent SQL injection attack commands more than 390 times into Marketwired's computer network and was able to steal more than 900 press releases.

B. Evidence of the Corrupt Trading

Analysis of the securities trading patterns of the defendants and their co-conspirators provides overwhelming evidence of the fact that they were trading in a highly coordinated manner based on MPNI that was unlawfully obtained and provided to them by the Hackers. Indeed, their trading patterns closely correlate to the periods of time prior to press release disclosures by the Victim Newswires.

Between January 2011 and February 2014 alone, the defendants and their co-conspirators executed approximately 1,000 inside the window trades based on MNPI stolen from the Victim Newswires resulting in approximately $30 million in illegal profits. Not surprisingly, the Traders were extremely successful when making these inside the window trades. Moreover, in instances when the Traders made inside the window trades that ultimately were not profitable, their trading patterns were consistent with the stolen MNPI but foiled by the vagaries of the market. For example, in August 2011, defendant Korchevsky and co-conspirator Arkadiy Dubovoy suffered combined losses of approximately $650,000 through inside the window trades on Sodastream International stock and approximately $270,000 through inside the window trades on Deere & Company stock. For both series of trades, Korchevsky and Arkadiy Dubovoy traded in the same direction "within the window," and their trades rationally, albeit unsuccessfully, applied the information in the press releases. For example, with the Sodastream trade, revenues and earnings per share beat expectations and the company had a record sales volume, but the shares nonetheless dropped.[6] Similarly with Deere & Company, the reported profits beat analyst expectations.

In addition, trading by defendants Korchevsky and Momotok occurred "within the window" before the disclosure of not only regular earnings reports, but also the disclosure

[5] "SQL Injection Attacks" are methods of hacking into and gaining unauthorized access to computers connected to the Internet.

[6] One market analyst later commented about Sodastream, "If you're a bit stunned by the market reaction, join the club. . . . . reacting as the market did is illogical."

of unscheduled press releases, meaning the defendants' trading sometimes corresponded to press releases that outside observers would have had no legitimate way of anticipating.

The investigation has also revealed that the defendants and their Trader co-conspirators coordinated with the Hackers to identify in advance particular companies that would likely be using the Victim Newswires to make public announcements that could be expected to affect those companies' stock prices. For example, on October 8, 2013, Pavel Dubovoy sent an email to Arkadiy Dubovoy with a blank subject line and attached a photograph of a printout of a spreadsheet that contained information about 18 U.S. publicly traded companies that were scheduled to issue press releases concerning earnings and other economically valuable information in October 2013. On October 9, 2013, Arkadiy Dubovoy forwarded this email to the defendant Garkusha. In October 2013, defendants Korchevsky and Momotok, together with Arkadiy Dubovoy, executed inside the window trades on six of the 18 companies listed in spreadsheet.

C. Evidence Linking the Defendants and their Co-conspirators

The evidence in this case demonstrates that the scheme's participants communicated frequently and extensively to coordinate their fraudulent inside the window trades to maximize profitability. They distributed stolen press releases in a variety of ways, including via email. For example, investigators executing a search warrant on a Yahoo! email account registered to defendant Khalupsky discovered a December 18, 2013 email containing an image of an unleased Oracle disclosure containing corporate earnings and other financial information.

The defendants and their co-conspirators also communicated via email and telephone to coordinate trading. For example, a Gmail email account registered to defendant Korchevsky exchanged numerous emails with a Gmail email account registered to conspirator Igor Dubovoy. On April 26, 2013, Igor Dubovoy sent an email to Korchevsky instructing him to sell their stock. In response, Korchevsky stated in an email that they "got the numbers right" but that the market's "reaction [was] mixed." Shortly after that email exchange, defendant Momotok began selling off stocks. In addition, that same day, Momotok and Igor Dubovoy contacted each other by telephone 22 times.

Similarly, on August 3, 2011, the press release for Dendreon Corp, which trades on the NASDAQ under the symbol "DNDN," was uploaded on a PR Newswire server at approximately 3:34 PM and issued to the public less than thirty minutes later at approximately 4:01 PM. Within this twenty-seven minute window, beginning at approximately 3:56 PM, defendant Korchevsky bought 1,100 put options of DNDN. The next day, Korchevsky sold all 1,100 put options for a profit of more than $2.3 million. Telephone records revealed that Korchevsky called Arkadiy Dubovoy's business on August 2, 2011, and again on August 3, 2011, before the DNDN press release was uploaded on PR Newswire. On August 4, 2011, after Korchevsky sold the put options, Korchevsky placed a call to and received a call from Arkadiy Dubovoy's business on two occasions.

The defendants and their co-conspirators also coordinated with the Hackers to distribute the unlawfully obtained proceeds of the scheme. For example, the Traders wired funds to accounts in Estonia, Macau and elsewhere in the names of shell companies controlled by the Hackers and the Traders. The Traders and Hackers also shared access to the same brokerage accounts. The IP address associated with conspirator Turchynov frequently accessed brokerage accounts controlled by Arkadiy Dubovoy and Igor Dubovoy that were used to execute hundreds of inside the window trades. Additionally, Arkadiy Dubovoy and Igor Dubovoy shared login and password information for brokerage accounts that they controlled with the defendant Khalupsky and an IP address associated with Khalupsky accessed these brokerage accounts on numerous occasions over the course of the conspiracy. Indeed, an IP address that was also used to unlawfully access one of the Victim Newswires successfully logged into trading accounts controlled by Arkadiy Dubovoy and Igor Dubovoy hundreds of times during the charged conspiracy.

Further, the defendant Korchevsky and the Dubovoys exfiltrated significant trading gains from the United States via money laundering havens in the Seychelles, British Virgin Islands, Panama, Belize and Ukraine. The Dubovoys and Korchevsky emailed wire instructions and account information to each other to coordinate their money laundering activities.

III. The Defendants

Vitaly Korchevsky, 50, is a naturalized United States citizen and resident of Glen Mills, Pennsylvania. Korchevsky has profited more than $17 million from this illegal scheme. He retains broad family connections to the Ukraine, where he was born and educated. Korchevsky has controlled brokerage accounts at E*TRADE, Fidelity and TD Ameritrade. Korchevsky has held numerous positions in the financial industry and was formerly a hedge fund manager and investment advisor who was registered with the Securities and Exchange Commission ("SEC") from 2005 through 2009. Most recently, Korchevsky was a Senior Vice President at Investment Counselors of Maryland, a boutique investment firm. Prior to that, Korchevsky was a Principal and Portfolio Manager at Victus/Vicis Capital. Prior to that, Korchevsky was a Vice President and Mutual Fund Manager at Gardner Lewis Asset Management, a money management fund that was purchased by Morgan Stanley. Thereafter, Korchevsky served as a vice president at Morgan Stanley.

Leonid Momotok, 47, a naturalized United States citizen and resident of Suwanee, Georgia, is a trader who is believed to be related to Igor Dubovoy and Pavel Dubovoy. Momotok shares an ownership interest in at least two of Arkadiy Dubovoy's companies and had formal trading authority for brokerage accounts used in this scheme but in the name of other members of the conspiracy, including Arkadiy Dubovoy. He profited at least $1.2 million from the scheme, and was given power of attorney by Pavel Dubovoy to trade in Pavel Dubovoy's brokerage accounts that realized approximately $5 million in illicit

profits. Momotok retains broad family connections to the Ukraine, where he was born and educated. Momotok controlled brokerage accounts at, inter alia, TD Ameritrade.

Alexander Garkusha, 47, a United States citizen and resident of Alpharetta and Cumming, Georgia, is an Executive Vice President at APD Developers, a company owned by Arkadiy Dubovoy. Garkusha also manages the trading operations of an entity which was used by Pavel Dubovoy to make payments to the Hackers. In addition, Garkusha was the former principal at Verum Capital Group LLC. Garkusha retains broad family connections to the Ukraine, where he was born and educated.

IV. The Charges

On August 5, 2015, a grand jury in the Eastern District of New York returned an indictment charging the defendants with conspiring to commit wire fraud, in violation of Title 18, United States Code, Section 1349; conspiring to commit securities fraud, in violation of Title 18, United States Code, Section 371; two counts of securities fraud, in violation of Title 15, United States Code, Sections 78j(b) and 78ff; and conspiring to commit money laundering, in violation of Title 18, United States Code, Section 1956(h).

THE DEFENDANTS SHOULD BE DETAINED

I. Legal Framework

Under the Bail Reform Act, Title 18, United States Code, Section 3141, et seq., federal courts are empowered to order a defendant's detention pending trial upon a determination that the defendant is either a danger to the community or a risk of flight. See 18 U.S.C. § 3142(e) (a judicial officer "shall" order detention if "no condition or combination of conditions would reasonably assure the appearance of the person as required and the safety of any other person and the community"). A finding of dangerousness must be supported by clear and convincing evidence. See United States v. Ferranti, 66 F.3d 540, 542 (2d Cir. 1995); United States v. Chimurenga, 760 F.2d 400, 405 (2d Cir. 1985). A finding of risk of flight must be supported by a preponderance of the evidence. See United States v. Jackson, 823 F.2d 4, 5 (2d Cir. 1987); Chimurenga, 760 F.2d at 405.

The Bail Reform Act lists the following factors to be considered in the detention analysis: (1) the nature and circumstances of the offenses charged; (2) the weight of the evidence against the defendant; (3) the history and characteristics of the defendant; and (4) the nature and seriousness of the danger to any person or the community that would be posed by the defendant's release. See 18 U.S.C. § 3142(g). The government addresses these factors below.

II. The Court Should Enter Permanent Orders of Detention for the Defendants

The factors considered in the detention analysis make clear that the defendants present an overwhelming risk of flight if released. Accordingly, the Court should enter permanent orders of detention pending trial for all the defendants.

A. The Nature and Circumstances of the Offenses Charged

The defendants and their co-conspirators operated a sophisticated, international, enormously profitable fraudulent criminal enterprise for more than five years. Through deception, the Hackers obtained unauthorized access to the Victim Newswires' computer networks and stole MPNI. The Hackers then disseminated the MPNI to the Traders, including the defendants, who used that information to realize fraudulent gains of approximately $30 million. Korchevsky personally profited more than $17 million from the scheme. These enormous sums of money could easily be used by the defendants to procure false identification documents and leave the United States.

Notably, the charged offenses carry significant terms of incarceration. If convicted of those charges, the defendants face statutory maximum prison terms of 85 years. If the defendants were convicted at trial on all counts, the government estimates their advisory sentencing range to be 235-293 months' incarceration. The prospect of spending decades in prison if convicted provides the defendants with a powerful incentive to flee.

B. The Weight of the Evidence

The weight of the evidence against the defendants is overwhelming. As described above, that evidence includes:

- the proceeds of numerous search warrants on email accounts and computer media seized by law enforcement officials both in the United States and overseas;
- telephone call logs and IP login records establishing the defendants' near-constant communications with each other and their co-conspirators;
- detailed trading records reflecting that defendants' carefully coordinated more than 1,000 inside the window trades and their disproportionate success in such trading, made possible through their possession of stolen MPNI;
- forensic artifacts of the Hackers' unauthorized intrusions into the networks of the Victim Newswires identified; and
- evidence of frequent communication between the Traders and the Hackers, including efforts to distribute the monetary proceeds of the illegal scheme.

Accordingly, this factor weighs heavily in favor of a finding that the defendants are likely to flee if they are released on bail.

C. The Defendants' Histories and Characteristics

The defendants' histories and characteristics further confirm that they present an overwhelming risk of flight. As described above, the defendants' scheme has generated approximately $30 million, most of which the defendants and their co-conspirators have successfully laundered outside the United States. Korchevsky personally profited more than $17 million, and Momotok profited approximately $1.2 million. These immense assets provide ready-made means for the defendants to orchestrate escapes to a non-extradition country.

Further, while the defendants are U.S. citizens, all have substantial familial ties to foreign countries and frequently travel overseas. For example, since this scheme began in 2010, Korchevsky has traveled outside the United States approximately 42 times, including multiple trips to Russia and Ukraine. During this same period, Garkusha has traveled outside the United States approximately 10 times. Momotok also has engaged in international travel. Indeed, Korchevsky returned to the United States earlier this month after spending several weeks overseas. They therefore represent an extreme risk of flight.

CONCLUSION

Through their illegal scheme, the defendants have access to millions of dollars in fraudulently obtained funds that they and their co-conspirators have secreted overseas. The defendants have strong overseas ties, and the means to escape to non-extradition countries. The evidence against them is overwhelming, and they face lengthy prison sentences if convicted. Accordingly, they represent substantial risks of flight.

For these reasons, the government requests that the Court issue permanent orders of detention for the defendants.

Respectfully submitted,

KELLY T. CURRIE
Acting United States Attorney

By: /s
Christopher A. Ott
Christopher L. Nasson
Richard M. Tucker
Assistant U.S. Attorneys
(718) 254-6154/6411/6204

cc: Counsel of Record (by hand and ECF)
Clerk of the Court (by ECF)
The Honorable Ramon E. Reyes, Jr. (by ECF)